Good evening hackers!! Today we will be doing a linux box named delivery. I am doing linux boxes first because linux is where I am most comfortable at. After I have exhausted linux boxes I will move to windows boxes. So lets not waste our time discussing these things and lets dive in!!

Enumeration

Kicking off with the nmap scan:

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:40:fa:85:9b:01:ac:ac:0e:bc:0c:19:51:8a:ee:27 (RSA)
|   256 5a:0c:c0:3b:9b:76:55:2e:6e:c4:f4:b9:5d:76:17:09 (ECDSA)
|_  256 b7:9d:f7:48:9d:a2:f2:76:30:fd:42:d3:35:3a:80:8c (ED25519)
80/tcp   open  http    nginx 1.14.2
|_http-title: Welcome
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.14.2
8065/tcp open  unknown
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest, SSLSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Accept-Ranges: bytes
|     Cache-Control: no-cache, max-age=31556926, public
|     Content-Length: 3108
|     Content-Security-Policy: frame-ancestors 'self'; script-src 'self'
cdn.rudderlabs.com
|     Content-Type: text/html; charset=utf-8
|     Last-Modified: Fri, 05 Nov 2021 19:51:59 GMT
|     X-Frame-Options: SAMEORIGIN
```

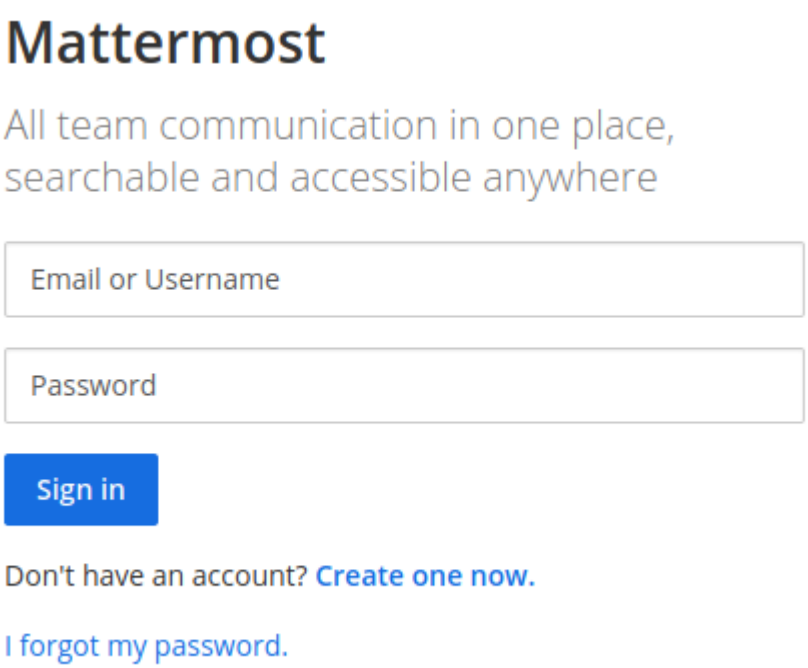
```
|     X-Request-Id: wdxwbn4hc7dgtp4n1bwjj3wpaa
|     X-Version-Id: 5.30.0.5.30.1.57fb31b889bf81d99d8af8176d4bbaaa.false
|     Date: Fri, 05 Nov 2021 20:04:08 GMT
|     <!doctype html><html lang="en"><head><meta charset="utf-8"><meta
name="viewport" content="width=device-width,initial-scale=1,maximum-
scale=1,user-scalable=0"><meta name="robots" content="noindex, nofollow"><meta
name="referrer" content="no-referrer"><title>Mattermost</title><meta
name="mobile-web-app-capable" content="yes"><meta name="application-name"
content="Mattermost"><meta name="format-detection" content="telephone=no"><link
re
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Date: Fri, 05 Nov 2021 20:04:08 GMT
|_    Content-Length: 0
```

From the scan we can note two important points. There might be some connection between the webservers or maybe one of them will be a rabbithole. So lets focus on port 8065 port first. Nmap wasn't able to detect the service version but from the output we can see nmap would have tried to fetch the version info but the server replied with a bad request. I tried to telnet the service, but the same 400 error code:

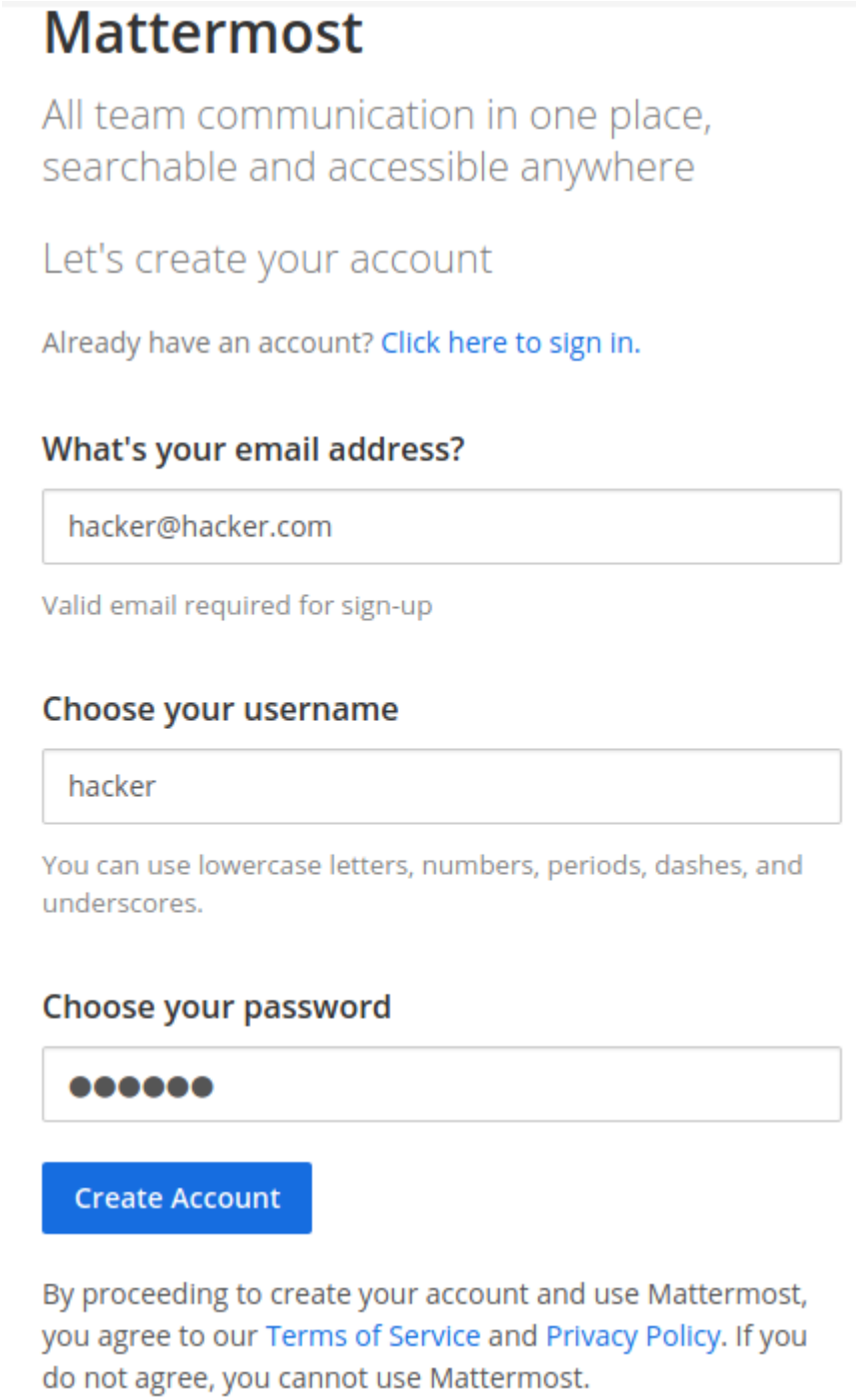
```
┌──(root💀kali)-[/home/rishabh/HTB/Delivery]
└─# telnet $IP 8065
Trying 10.129.251.190...
Connected to 10.129.251.190.
Escape character is '^]'.
id
HTTP/1.1 400 Bad Request
Content-Type: text/plain; charset=utf-8
Connection: close

400 Bad RequestConnection closed by foreign host.
```

So without wasting further time, I launched firefox and went to port 8065

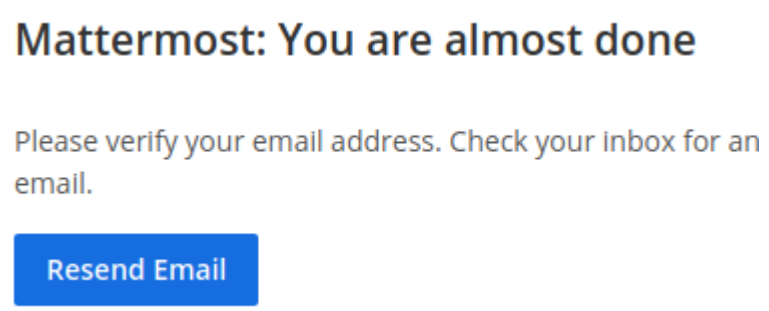
Port 8065



Its running a login page for a open-source chat service where you can collaborate with other team members. In simple words, its an alternative to Microsoft Teams. My first step would be to look at wappalyzer output and see if there are any other info and running plugins in this website. Unfortunately, it didn't recognize any. Next easy win is I went to reviewing source code and even it didn't contain any sensitive info. I went to robots.txt but no sensitive disallow entry. I googled default credentials for mattermost but no luck again. Both username and password is set during configuration and it is present in config.json file. There was also a create account feature so I created a quick account to enumerate more as a low level user. LOL. It seems they are playing with us:



I put random email and I must admit they follow strict password requirements, they sent a confirmation email. It seems, this might be the end for this service enumeration. Possibility is there are credentials hidden in other service which will come handy for this service further.

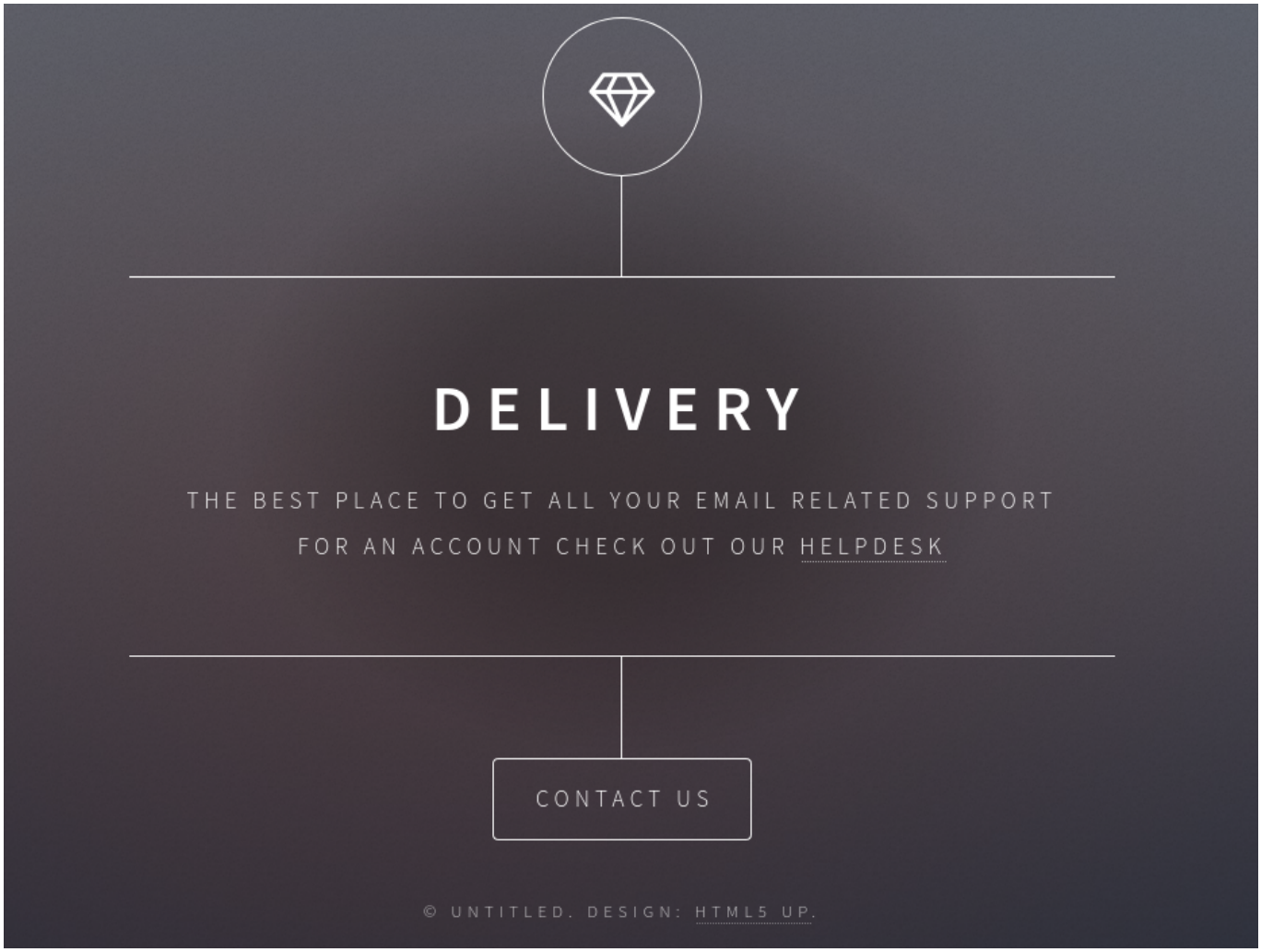


Also I left a gobuster scan in the background while I enumerate port 80.

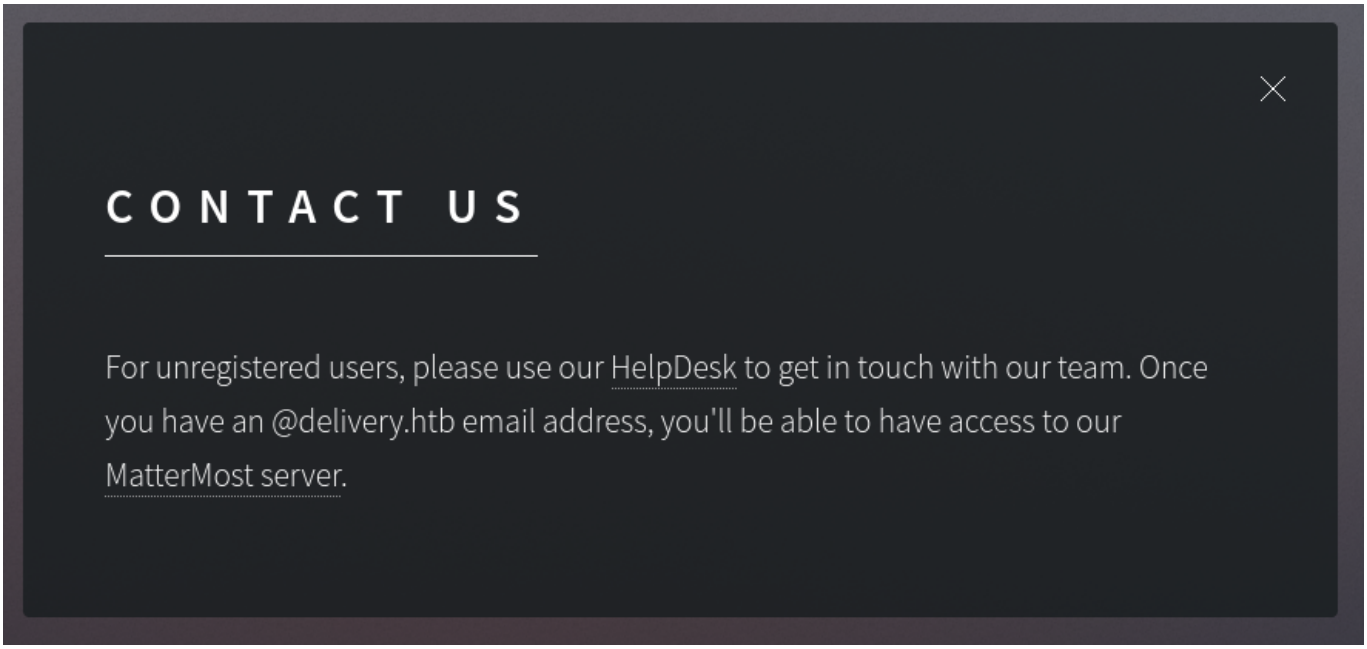
```
┌──(root💀kali)-[/home/rishabh/HTB/Delivery]
└─# gobuster dir -u http://$IP:8065/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20
0 --no-error -o dirbust -b 400,404 -q --exclude-length 3108,0
```

Probably there's nothing much more to enumerate here.

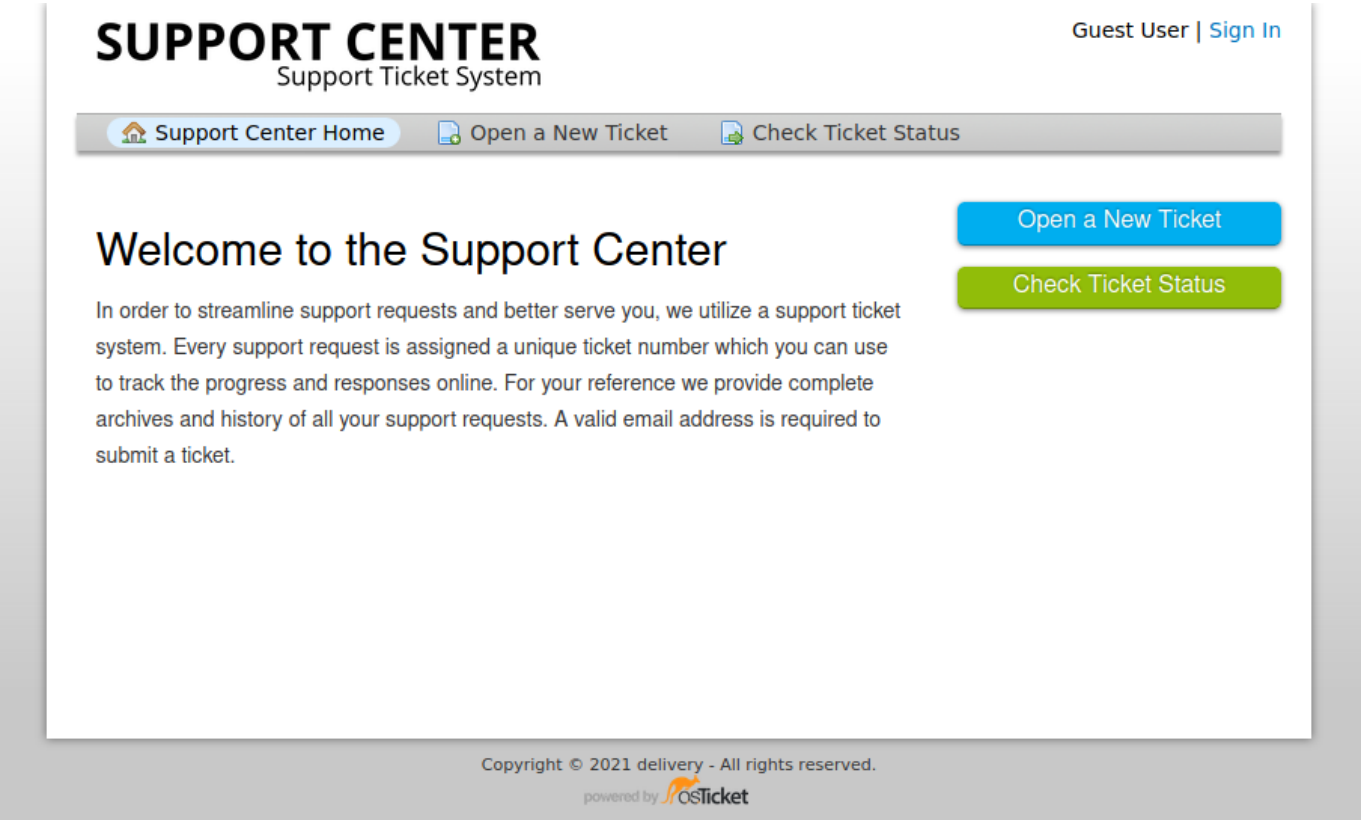
Port 80



A nicely designed website probably nothing much to do except one link which gets navigated to "helpdesk.delivery.htb" and a contact us box which gets displayed if you click on contact us at the bottom.



I quickly added this entry and also delivery.htb to my hosts file. Restart your browser and navigate to helpdesk.delivery.htb

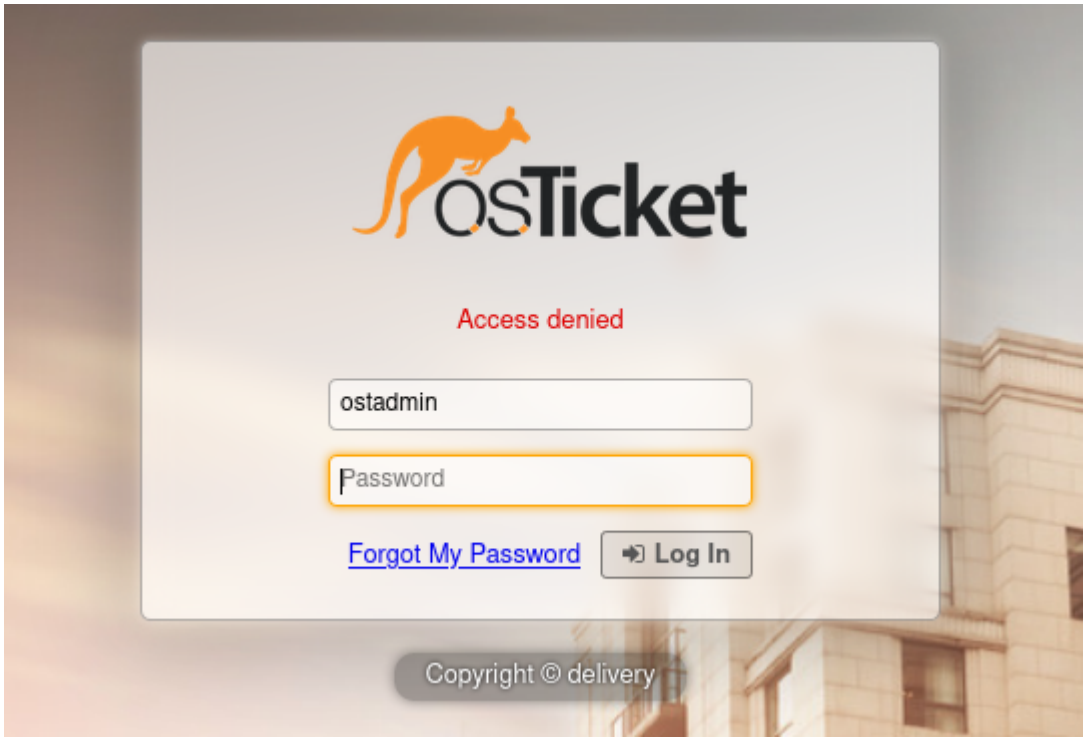


Its an Issue tracker system by OSticket. Also, wappalyzer shows its running php as

programming languages which indicates we might be needing a php reverse shell. Right now we don't have any version info too. I googled for default credentials of OSticket and they showed me this:

> Wait for the installation to complete then browse to your OSTicket staff control panel at http://localhost:8080/scp . Login with default admin user & password: **username: ostadmin**. **password: Admin1**.

There's a staff control panel directory(scp) where you can login with admin credentials.

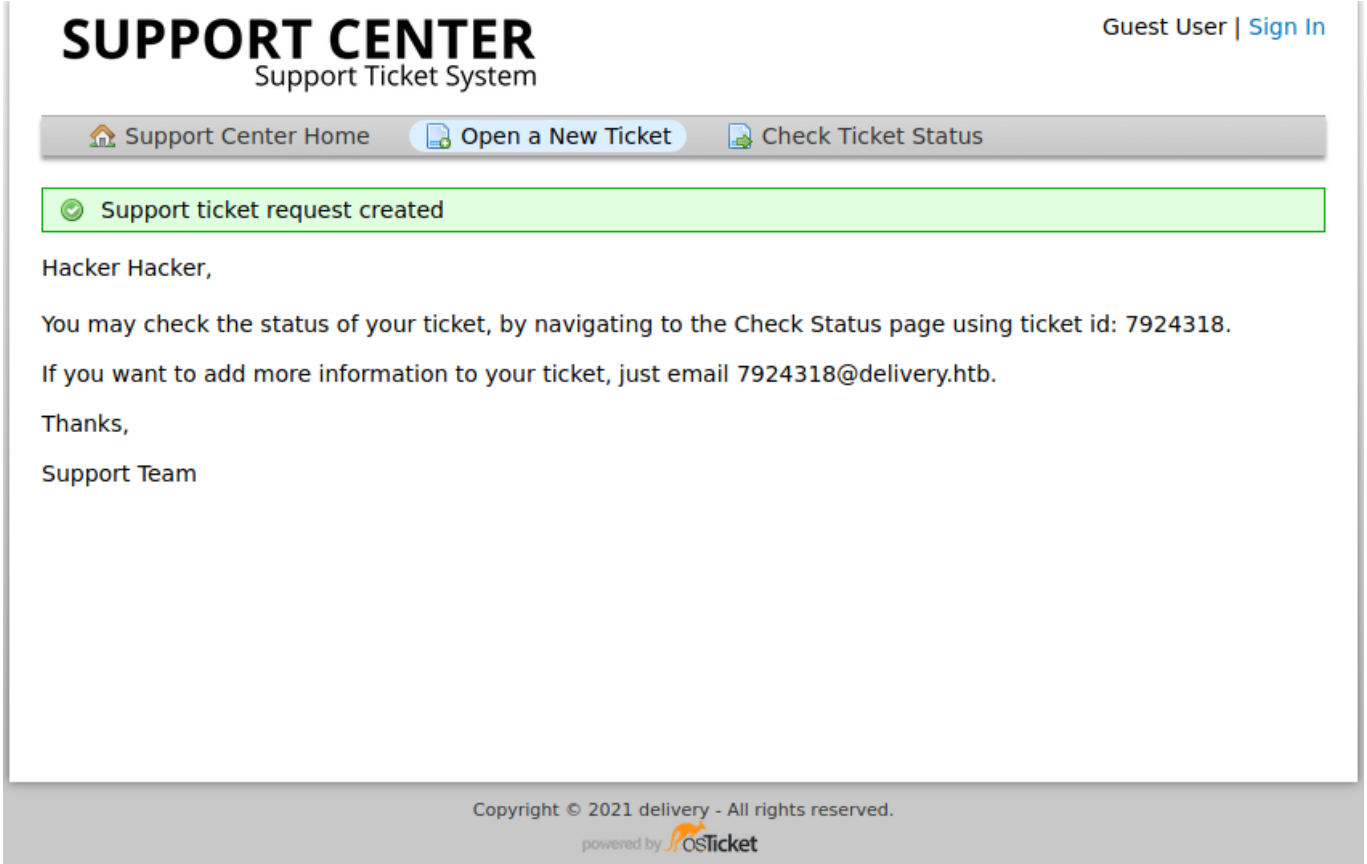


Unfortunately default creds didn't work and if you try to login too many times with a wrong password, you might reach max tries reached and probably your IP will get blocked (happens in realistic scenario). So bruteforce is out of the way. I tried very easy passwords like [password, admin, administrator, osticket, delivery, Admin1] but all failed. I read the source code but again no luck. I finally read directory brute forcing tool named gobuster to do some work for me. Meanwhile, I even ran a subdomain bruteforce just not to leave any stone unturned. Subdomain scan didn't give any positive result other than helpdesk which we already know but we do have many subdirectories and files to check for any hidden info.

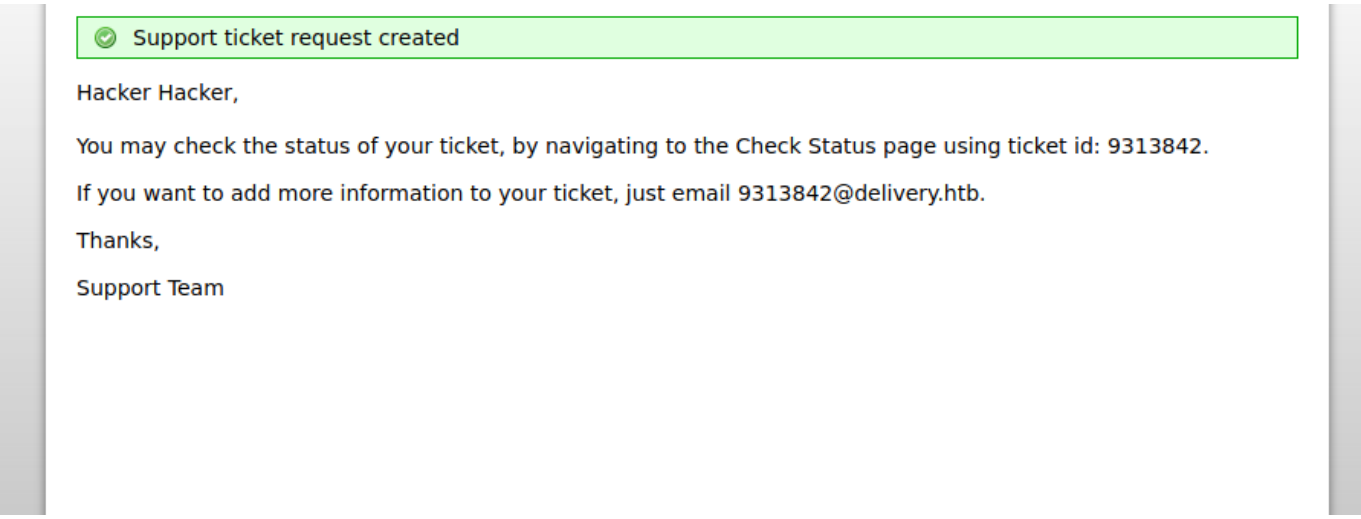
```
┌──(root💀kali)-[/home/rishabh/HTB/Delivery]
└─# gobuster dir -u http://helpdesk.delivery.htb/ -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 200
--no-error -o dirbust_2 -b 400,403,404,502 -q -x php,txt
/pages                (Status: 301) [Size: 185] [-->
```

```
http://helpdesk.delivery.htb/pages/]
/images                 (Status: 301) [Size: 185] [-->
http://helpdesk.delivery.htb/images/]
/profile.php            (Status: 422) [Size: 5181]
/index.php              (Status: 200) [Size: 4933]
/logo.php               (Status: 302) [Size: 0] [-->

/assets/default/images/logo.png]
/apps                   (Status: 301) [Size: 185] [-->
http://helpdesk.delivery.htb/apps/]
/view.php               (Status: 200) [Size: 5263]
/assets                 (Status: 301) [Size: 185] [-->
http://helpdesk.delivery.htb/assets/]
/account.php            (Status: 200) [Size: 37319]
/css                    (Status: 301) [Size: 185] [-->
http://helpdesk.delivery.htb/css/]
/js                     (Status: 301) [Size: 185] [-->
http://helpdesk.delivery.htb/js/]
/kb                     (Status: 301) [Size: 185] [-->
http://helpdesk.delivery.htb/kb/]
/api                    (Status: 301) [Size: 185] [-->
http://helpdesk.delivery.htb/api/]
/open.php               (Status: 200) [Size: 8133]
/manage.php             (Status: 200) [Size: 63]
/tickets.php            (Status: 422) [Size: 5181]
/captcha.php            (Status: 200) [Size: 4329]
/scp                    (Status: 301) [Size: 185] [-->
http://helpdesk.delivery.htb/scp/]
/offline.php            (Status: 302) [Size: 0] [--> index.php]
/bootstrap.php          (Status: 200) [Size: 0]
```

Any syntax related questions, pls refer tool's help page. Many of the above results were false positives. Running out of ideas, I registered for a fake account, but if you login with those creds, account confirmation will be required. I even creted a ticket using guest user, inserted a link to "google.com" just for understanding the workflow, a ticket ID will be generated which you can access after logging in.

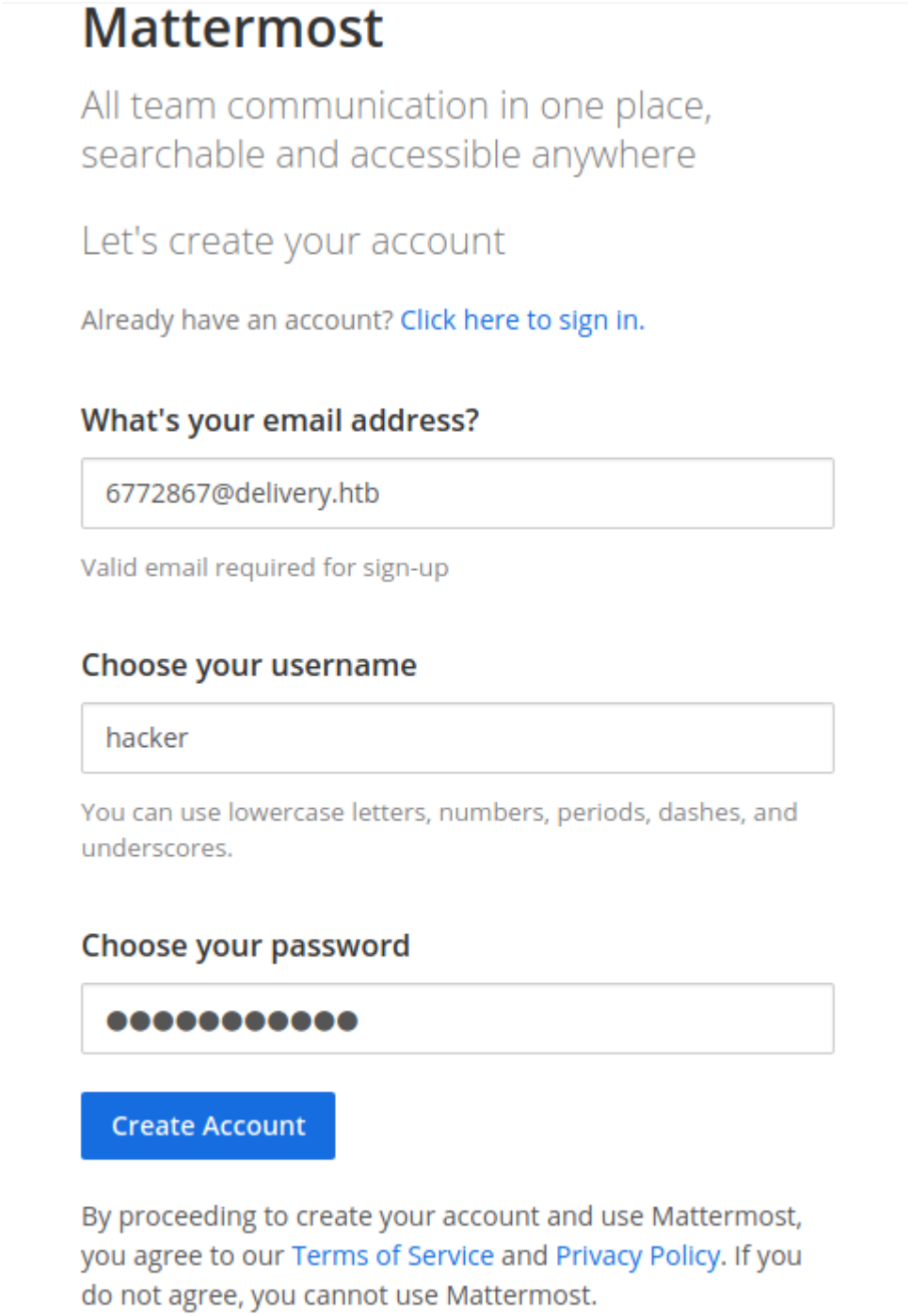


I googled for osticket exploits but most of them were showing XSS which isin't use to us. I just peaked a little at one of the walkthroughs, Sorry, and I seriously wanted to hit myself after that seeing that hint. The contact us box which we found earlier was a hint. We need email@delivery.htb type email address so that we can log in to MatterMost server. Also, if you open a ticket as a email@delivery.htb, you get a ticket id, and a ticketid@delivery.com type email address. Now as a guest user, create a ticket and keep note of the ticket id:

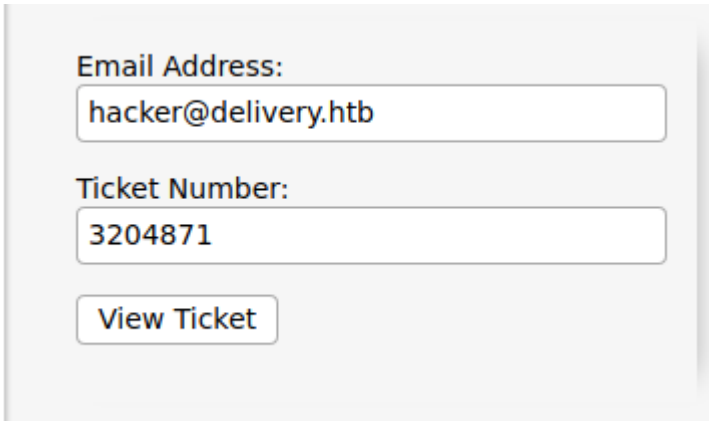


In the message which you get from support team, its written "If you want to add more information to your ticket, just email ticketID@delivery.htb" . I hope you guys are getting a

clue what I am about to do next.
Now go to mattermost page, click on create account, use the email address you have got from support team.

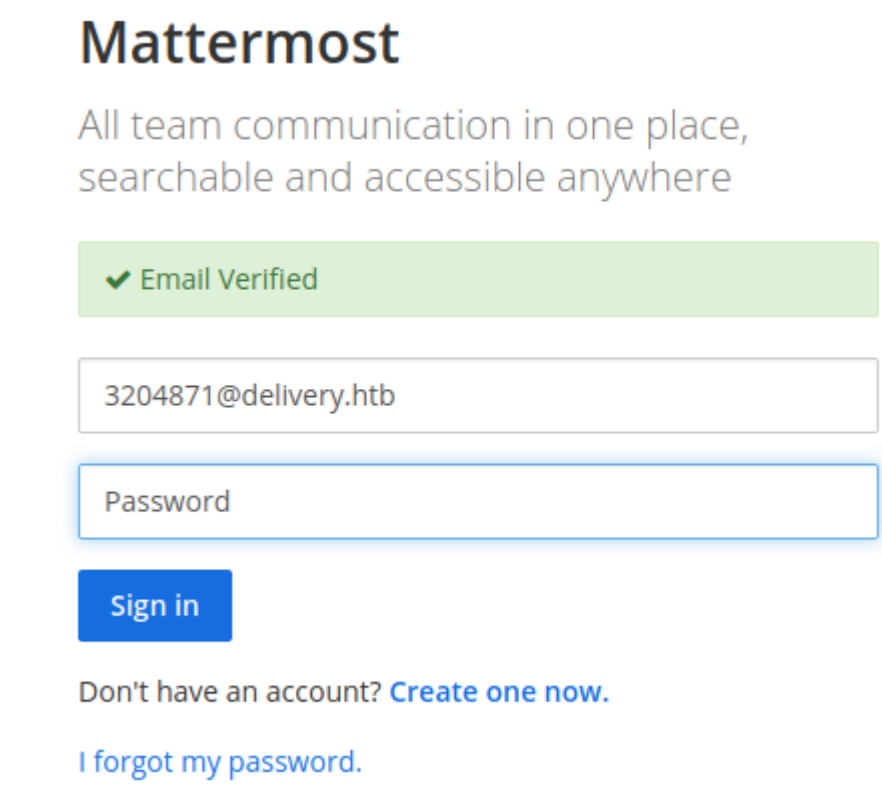


Now, click on Check ticket status, use the email address you used to create a ticket and enter ticket id:

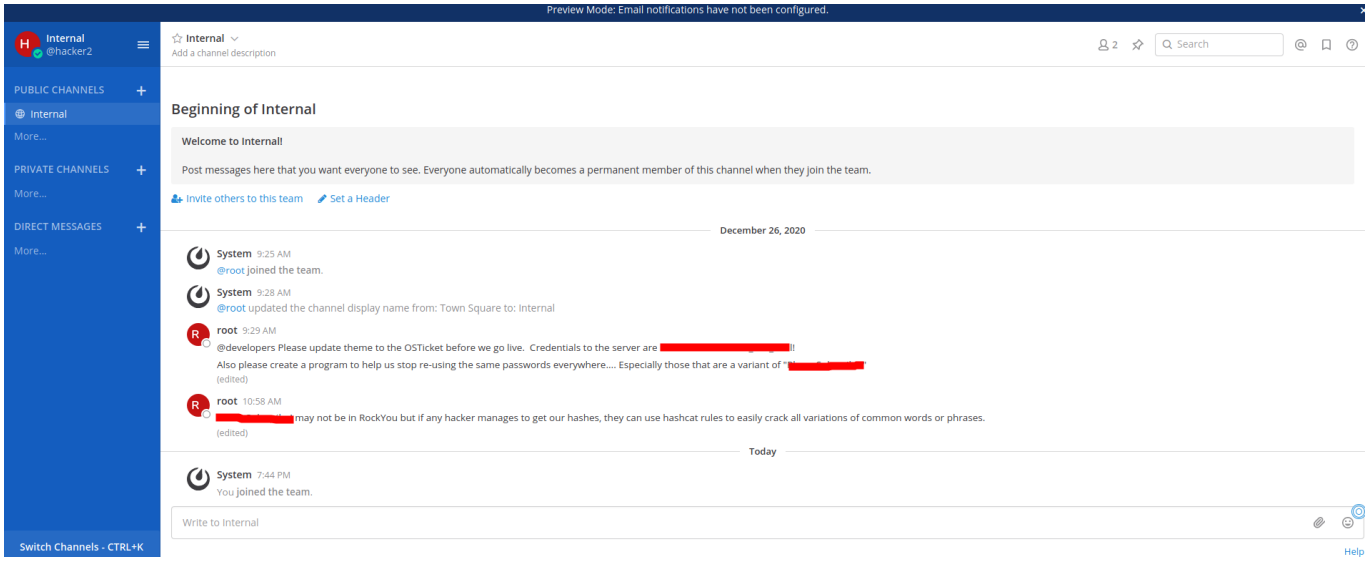


You would have got something like this:

---- Registration Successful ---- Please activate your email by going to: http://delivery.htb:8065 /do_verify_email?token=6rtiened3gsf7t4cuguw3a1zjm8ty5r1444ko4dhah977ezjqxzh83nuthojzrft& email=3204871%40delivery.htb) ---------- You can sign in from: ---------- Mattermost lets you share messages and files from your PC or phone, with instant search and archiving. For the best experience, download the apps for PC, Mac, iOS and Android from: https://mattermost.com/download/#mattermostApps (https://mattermost.com/download/#mattermostApps



Enter the password and you are in:



This is the internal channel which will be open by default after skipping the tutorial, I have redacted the credentials which will help us in our next step. Using the credentials found go to the scp directory in the osticket webpage and enter those credentials and it worked.

Initial Access

I again used that username and password to ssh into the machine and I was able to log in.

```
┌──(root💀kali)-[/home/rishabh/HTB/Delivery]
└─# ssh maildeliverer@$IP
maildeliverer@10.129.251.190's password:
Linux Delivery 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jan  5 06:09:50 2021 from 10.10.14.5
maildeliverer@Delivery:~$
```

Privilege Escalation

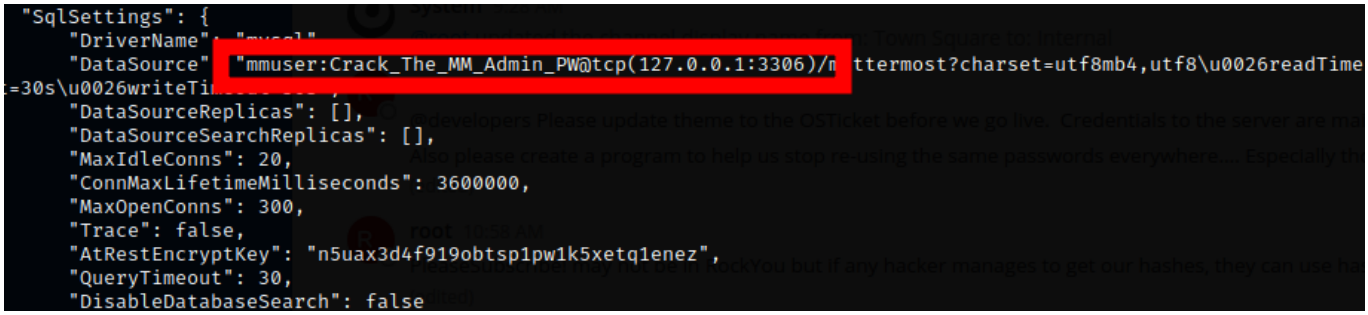
Without wasting my time, I transferred linpeas and let it do the work for me. From the output, I collected three important things:

```
root       972  0.0  0.4  29528 18208 ?        S    15:52   0:00 python3 /root/py-smtp.py
```

```
 85M -rwxrwxr-x 1 mattermost mattermost  85M Dec 18  2020 /opt/mattermost/bin/mattermost
```

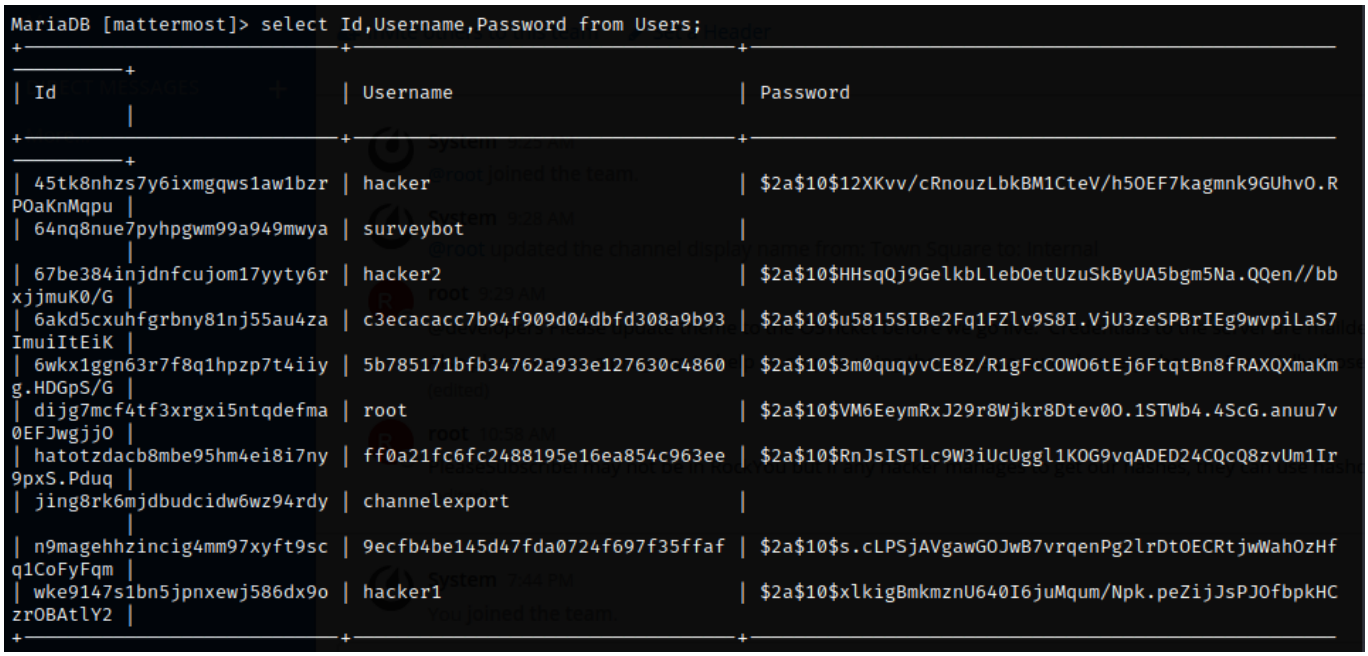
```
* * * * *       root    /root/mail.sh
```

Cron job will surely come handy later but for now both root files can't be read or accessed. I went with mattermost and as I told you earlier, mattermost keeps its confirguration info in config.json file. So lets see what it has to offer.
In sql settings you will see credentials in this format username:password@tcp(127.0.0.1:3306):



So we have our username and password. Login to mysql locally using this command:

```
mysql -u mmuser -p
```



There it is, root hash. I copied the hash and threw it to john but it was unsuccessful. I went back and read the thread again by root "Also please create a program to help us

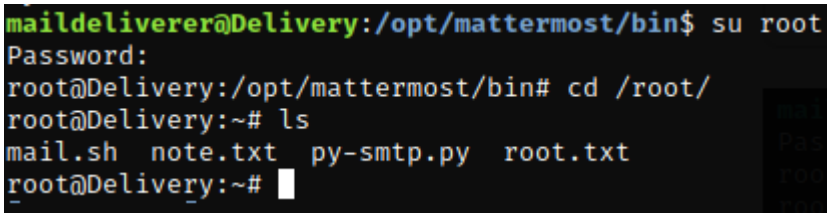
stop re-using the same passwords everywhere.... Especially those that are a variant of 'PleaseSubscribe!'" . We can infer from this statement that the password must be some variant of this word. Also, in the end root mentions about hashcat rules which can be used to generate variations and then we will use john to crack the root hash we got earlier. As I am running a virtual machine, hashcat doesn't run on my VM, so I cheated here a little bit. If you want to know whats the process here it goes:

```
hashcat -r /usr/share/hashcat/rules/best64.rule --stdout file > dict.txt
```

Here "file" contains "PleaseSubscribe!" and all the variants will be written to dict.txt and also hashcat is using a rules file with -r switch.

```
john --wordlist=dict.txt hash
```

John will crack the password in no time. Enter the password and you are root.



Voila!! You are root. It wasn't an easy machine, specially for the first time, there weren't any use of exploits. It was all enumeration and joining the dots. Also, its a great machine for learning hashcat. I will learn hashcat on my windows host soon. LOL. I am a john fan. Anyways cheers and happy hacking!!